Open Source Vulnerabilities and License Risks:

Visibility Sooner

WHAT ARE OPEN SOURCE VULNERABILITIES?

Open source vulnerabilities are introduced through weaknesses in the code or capability that can be exploited accidentally by bugs or via malicious packages crafted by cybercriminals.

Gartner

Open Source used in more than 90% of IT organizations worldwide

snyk

2.5x increase in open source vulnerabilities since 2017

4 OVERLOOKED OPEN SOURCE RISKS

1. Public libraries
2. Difficult to track compromised code
3. Rights infringements
4. Human error

snyk

Many open source vulnerabilities continue to be discovered in indirect dependencies:

- NPM: **86%** of vulnerabilities are indirect dependencies
- RUBY: **81%** of vulnerabilities are indirect dependencies
- JAVA: **74%** of vulnerabilities are indirect dependencies

WHAT ARE THE IMPACTS?

When hackers exploit an open source vulnerability, they can gain access to troves of sensitive data being stored within the application. Here's how a data breach impacts organizations:

BUSINESS DAMAGE AND LOSS OF MARKET

Arkose Lab study: **50%** of companies polled lost customers due to breaches, regardless of industry or size

INCURRED COSTS AND FINANCIAL LOSS

Equifax settled a class-action lawsuit for **USD $380.5 million** due to a breach via open source vulnerability

COMPLIANCE PENALTIES AND LOSS OF INTELLECTUAL PROPERTY

PCI-DSS:
USD $5,000 to $100,000 per month until resolved

GDPR:
4% of total global turnover or $20 million euros

HIPAA:
Max USD $1.5 million fine per incident

CURRENT OPEN SOURCE VULNERABILITIES:

HTTPS

CVE-2014-0160
Hundreds of millions of websites were affected by a serious vulnerability dubbed Heartbleed

CVE-2017-5638
Hackers exploited the Apache Struts² framework in the Equifax breach

CVE-2017-16095
Used by 4.35 million GitHub projects and affected all versions of the popular npm Lodash library

HOW LONG DOES IT TAKE TO REMEDIATE VULNERABILITIES?

The honest answer?
Too long. According to Snyk, remediation timelines don't match with community expectations.

- **36%** FIXED AFTER 70 DAYS
- **29%** FIXED 20-70 DAYS
- **34%** FIXED <20 DAYS
- **1%** FIXED SAME DAY

HOW SECOPS CAN MANAGE OPEN SOURCE RISKS:

- Select a purpose built tool that integrates with your DevOps infrastructure
- Track dependencies and monitor deployed code
- Prioritize critical vulnerabilities
- Manage open source licenses
- Implement security efficiencies

TREND MICRO CLOUD ONE™ – OPEN SOURCE SECURITY BY SNYK CAN HELP:

Trend Micro has partnered with Snyk to create the first purpose-built service for SecOps teams. As part of the Trend Micro Cloud One™ security services platform, the solution connects with your code repositories and CI/CD pipelines, allowing you to:

- Scan projects in code repositories to gain visibility into open source dependency vulnerabilities
- Generate an automated open source bill of materials report of vulnerabilities and license risks from one place
- Gain deeper insight into all your applications for better risk management of open source issues
- Unified SaaS security platform with single sign on, flexible procurement and billing, and broad integration support

Test your projects for open source vulnerabilities directly from your repository

Try it for free

Click here to get started and test up to 15 projects for free